# Generation of Anonymous Signature and Message using Identity Based Group Blind Signature

S.Kuzhalvaimozhi [1] , Dr.G.Raghavendra Rao[2]
[1] National Institute of Engineering, Mysore, Karnataka – 570008. Email : kuzhali_mozhi@yahoo.com
[2] National Institute of Engineering, Mysore, Karnataka – 570008. Email : grrao56@gmail.com

***Abstract*— The essential functionality of any digital transaction system is the protection of the anonymity of user and the message. Group signature allows any valid group member to sign any number of messages on behalf of the group without revealing the member identity. A blind signature is a cryptographic scheme produces a signature, where the digital signature is obtained on a message from a signer without revealing any information about the message. In this paper we bring in a new cryptographic scheme called a Group Blind Digital Signature combines the existing concept of a Group Digital Signature and a Blind Digital Signature. This scheme is useful in many applications where anonymity is very important like evoting and ecash. This blind group signature scheme uses the identity based signature in which the public key can be derived from any arbitrary unique string. This reduces the complexity involved in certificate management as compared to the traditional public key signature scheme. Moreover, this signature scheme based on the bilinear pairings enables utilizing smaller key sizes**

*Index Terms*— **Digital signature, Group Signature, Blind Signature, Bilinear Pairing**

## I. Introduction

A Group Blind Digital Signature allows the members of a group to digitally sign documents on behalf of a group and also the signer is unaware of the message that he is signing. The purpose of the digital signature is to enable a person to digitally sign the electronic document. The digital signatures have the same properties as traditional signatures. The digital signatures are easy to generate, easy to verify. However they are difficult to forge. To sign a document, private key is used, and the public key is used for verification. Digital signatures have extensively been used to offer services such as data integrity, entity authentication, non-repudiation, and data origin authentication.

### *A. Group signature*

Group signatures, allows a group member to anonymously sign on behalf of the group[5,11,12]. Using a single group public key, the signatures can be verified. It is impossible for anyone to distinguish whether or not two group-signatures originated by the same or by a different group member. In the case of a disagreement, only the designated group manager can open the signature to disclose the identity of the group member who issued the given signature. Group signatures[14] are publicly verifiable and can be verified with respect to a single group public key.

Group signatures have many applications in the area of privacy protection [7,9]. The most well-known one is trust computing. Since the number of applications on the internet continues to grow, more and more conventional human interactions have been transformed to their electronic transactions like email, ecash, evoting, ecommerce, etc[8,13]. In the electronic transaction environment the personal privacy is a big challenge, like the right of the individual is much less or the right to find out the amount of personal information which should be available to others is more.

Privacy is important for many reasons, such as impersonation and fraud. It becomes easier for criminals to commit fraud as more identity information is collected, correlated, and sold. But privacy is more than that, it also concerns about the secrecy of which websites we visited, the candidates we voted for, etc. Anonymity is one important form of privacy protection.

For some application high level of anonymity can do more damage. For example, in some situation one would like to have a trusted third party to have the capability to trace users after the fact that users have misbehaved, such as tracing double-spenders in an electronic cash system. Designing secure cryptographic schemes with unconditional anonymity is undoubtedly challenging. In practice, anonymity diversifies into various forms with different levels of anonymity. However, providing the proper level of anonymity is sometimes even more challenging.

### *B. Blind signature*

With the vast development of electronic commerce, the protection of anonymity of users and messages become a crucial requirement. The best approach to authenticate any e-transactions is the digital signature, which allows a user with a public key and a corresponding private key to sign a document in such a way that anyone can verify the signature on the document, but no one can fake the signature on any other document. Blind signatures are the basic tool for secured electronic transactions.

A blind signature is similar to a digital signature, a user can obtain a signature from a signer, but at the same time the signer of the message does not find out the information about the message they signed. Moreover, should the signer ever see the document or signature pair, he/she should not be able to determine when or for whom he signed it.

## II. Related work

The first Group Signature proposed by Chaum and van Heyst[4]. In this scheme the signer is a member of the group

© 2013 ACEEE
DOI: 01.IJNS.4.1.1133

signer’s identity is hidden in a group, but the group’s identity is revealed. Besides the first realization Chaum and van Heyst proposed, there are many other schemes emerge in recent years. G. Ateniese[8] proposed a group signature scheme based on other number theory assumptions with better efficiency and stronger security. More researches on group signature include group signatures for hierarchical multi-groups, group blind signatures, and multi-group signature.

Blind signature was first introduced by Chaum [3], which can provide anonymity for users in electronic transactions. It allows users to get a signature of a message in a way that signer learns neither the message nor the resulting signature. Chaum first proposed blind signature scheme was RSA-based. The first ID-based blind signature scheme [6] was proposed by Zhang and Kim in 2002. After that, there have been several proposals for the blind signatures. Many research papers provide the details of digital signature scheme which comprise blind signature and signcryption schemes using identity based cryptography system. In this paper, we construct a provably secure ID-based group blind signature on the basis of CZK scheme.

## III. Preliminaries

Here in this section, we briefly present the background concepts which help in understanding the Identity-based Group Blind signature systems.

### *A. Identity Based Cryptosystem*

In recent years the Identity-based cryptosystems are becoming popular. The advantage of Identity Based Encryption (IBE) system is that users can choose any arbitrary string as their public key [1, 15]. IBE goal is to reduce the overhead necessary to bring an entity into the crypto system. We take some attribute of the entity and use that as a functional equivalent to a public key. Thus, a name, an email address, or even a binary object such as a picture or sound can be considered equivalent to a public key. An IBE system can be thought of as a function of the form Ki = IBE(IDi) that produces keys from arbitrary bit strings. This reduces the overhead of using of certificates [2,10,15] in the traditional public key infrastructure.

### *B. Identity Based Signature Scheme*

In Identity Based Signature Scheme (IBS), the sender obtains a private key associated with the unique identity information from the PKG. Then the sender signs a message using the signing key. The verifier uses the sender’s identity information to verify the signature. For the verifier it is not required to get the sender’s certificate to verify the key[1]. More precisely, an IBS scheme can be described using the following steps.

– Setup: The Private Key Generator (PKG), which is a trusted third party, creates its master private and public key pair.
– Private Key Extraction: The sender authenticates to the PKG and obtains a private key associated with the identity.
– Signature Generation: Using the private key, the sender creates a signature on the message M.
– Signature Verification: Having obtained the signature and the message M from sender, the verifier checks whether the signature is a genuine signature on M using sender’s identity and the PKG’s public key. If it is, then the receiver accepts the message or otherwise rejects it.

### *C. Bilinear Pairing*

Bilinear pairing is an important primitive for many cryptographic schemes. Many elegant cryptographic schemes have been formulated utilizing the properties of these bilinear pairings.

Let $G_1$ be an additive group of prime order q, generated by P, and let $G_2$ be a multiplicative group with the same order q. We assume that there is a bilinear map e from $G_1 \times G_1$’! $G_2$ with the following properties:

*1) Bilinearity:*

Which means that given elements,
$A_1, A_2, A_3 \in G_1$ , we have that
$e(A_1 + A_2, A_3) = e(A_1,A_3) \times e(A_2,A_3)$ and
$e(A_1, A_2 + A_3) = e(A_1, A_2) \times e(A_1, A_3)$.

In particular, for $e(aA_1, bA_2) = e(A_1, A_2)^{ab}$, a,b ε $Z^*q$ where Zp denotes all positive integer which is less than p. $Z^*q$ denotes multiplicative group modulo p.

*2) Non-degeneracy:*

Which means that there exists $A_1, A_2$ ε $G_1$ such that $e(A_{1,} A_2) \neq 1_{G2}$, where $1_{G2}$ is the identity of $G_2$.

*3) Computability:*

Which means that there exists an efficient algorithm to compute e(A1, A2), “ A1, A2 ε $G_1$.

*Decision Diffie-Hellman is easy:* The Decision Diffie-Hellman problem (DDH). Given aP, bP, cP ε $G_1$. If we want to decide whether cP = abP, we can easily determine by checking e(P, cP) = e(aP, bP).

Computational Diffie-Hellman is hard: The Computational Diffie-Hellman problem (CDH). Given P, aP, bP ε $G_1$, if we want to compute abP ε $G_1$, it is assume to be hard.

Since the Decision Diffie-Hellman problem (DDH) in $G_1$ is easy, we cannot use DDH to build our cryptosystems. Instead, the security of our IBE system is based on a variant of the Computational Diffie-Hellman assumption (CDH).

### *D. Properties of Group Blind Signature*

A secure group signature scheme satisfies the following properties:

1) Anonymity: For given a signature, identifying the real signer is infeasible to decide for everyone but the group manager.
2) Blindness: The signer is unable to see the original content of message he/she has sign.
3) Unlinkability: Deciding whether two different signatures made by the same signer is computationally hard.
4) Unforgeability: Only group members can sign messages on behalf of the group.
5) Correctness: Signature produces by a group member must be provable.

DOI: 01.IJNS.4.1.1133

6) No framing: The group members/manager can not sign messages for other members.

7) Traceability: The group manager can always establish the identity of the member who issued a valid signature.

8) Exculpability: Even if the group manager and some of the group members join together, they cannot sign on behalf of non-involved group members.

## IV. Identity Based Group Blind Signature

In this paper we investigated the generation of Group blind signature with identity based cryptosystem. An identity based Group blind signature scheme is an interactive procedure allowing Sender to obtain a valid signature for a message from a signer without seeing the message or its signature.

In this section we present how an Identity based signature scheme can be used to implement an efficient group signature scheme. In this scheme all users get a private key from the Group Manager using system parameter. This group signature scheme involves three types of parties: members, non-members and a group manager. It further consists of seven algorithms Setup, Member key generation, Join, Signing, Verifying, Open, and Signer Tracing as shown in Figure 1. The blind group signature scheme is composed of the following procedures:

***Setup*:** In this algorithm the Group Manager (GM) chooses the input of security parameters and a group secret key of the group manager and output a group public key.

Let G1 be acyclic additive group of prime order q generated buy P, G2 be a cyclic multiplicative group of the same prime order q. A bilinear pairings is a map ê: G1×G1→ G2. The GM decides on a bilinear pairing e and P an arbitrary generator of $G_1$.

- GM selects a Map to point hash function $H_1$: {0, 1}* × G1 → $Z_q$* and
- Chooses another cryptographic hash function $H_2$: {0,1}* × G1→ G1
- $H_1$,$H_2$are secure one-way hash functions.
- GM chooses a generator P of G1
- Selects a random s $^a$ $Z_q$*
- Computes $P_{pub}$ = sP.
- Group public key is $G_{pub}$ = (P, $P_{pub}$, ê, q, G1, G2, $H_1$, $H_2$).
- GM Secret key is
- GM publishes the system parameters ($G_{pub}$) and keeps the master key as secret.

*Member key generation:* Any group member wants to generate his/her member secret key, they uses the interactive protocol with the group manager. During which Group Manager generates a member certificate on the member secret key blindly, i.e., without knowing the secret key value. Any group member can generate group signatures using his member secret key and member certificate, called group signing key. The communication between the GM and the group member is secured. To acquire the membership certificate, each user must execute the following protocol with GM:

- The group member with identity $ID_i$ selects a random number $r \in Z_q{}^*$ as the private key.
- Computes rP and the group member send rP together with $\boldsymbol{ID_i}$ to GM.
- GM computes group member's private key

$$S_{ID_i} = s \,.\, H_2(ID_i \,||\, rP)$$

- Sends $S_{ID\,i}$ to the group member via a secure channel.
- The group member has a private key $pair\ (r, S_{ID_i})$ .( $S_{ID\,i}$ and rP are pseudo-secret, since GM is no longer trustful and it may expose them to other members.)
- Group member's public key $Q_{ID_i} = H_2(ID_i \,||\, rP)$

***Join:*** Suppose now that a user wants to join the group performs the following protocol and becomes a member of the group.

- User chooses a random $x \in Z_q{}^*$
- Sends $\{rxP, rP, ID_i, xP\}$ to GM and proves to GM that the user knows $S_{ID\,i}$.
- If GM is convinced that the user knows $S_{IDi}$ and $\hat{e}(xP, rP)$
- GM sends secretly $S = sH_2(\,rxP)$
- User has the secret keys ***x and rx***, member key ***xP***, and the member certificates (***rxP, S***).

***Signing:***

This algorithm includes many phases like initializing random value, blinding message, signing the blinded message and unblinding.

During initializing phase the signer initializes a random value and sends to the user. The user then calculates the blinding factore using the random value and other parameters. The blinded message is send to the signer for signing. After signing the user unblinds the signed message by sending the blinding factor to the verifier.

Signer:

- Chooses randomly $\boldsymbol{k_1}$ "$\boldsymbol{Z^*_q}$
- computes $\boldsymbol{R_1} = \mathbf{k_1} \cdot \boldsymbol{H_2(rxP)}$
- sends $\boldsymbol{R_1}$ to the sender.

Sender:

- Chooses randomly ***bfact*** " $\boldsymbol{Z^*_q}$
- computes and sends $\boldsymbol{R_2 = R_1 + bfact \cdot P}$
- calculates $\boldsymbol{R_3 = H_2(m, R_2)}$
- sends $\boldsymbol{R_2}$ and $\boldsymbol{R_3}$ to signer

Signer:

- computes $\boldsymbol{R_4 = rx \cdot R_3}$
- sends $\boldsymbol{R_4}$ to sender

Sender : In this phase the signer blinds the message with the blind factor.

- computes $\boldsymbol{R_5 = R_4 + bfact \cdot P}$
- computes $\boldsymbol{R_6 = H_1(m, R_2 + R_5)}$
- sends $\boldsymbol{R_6}$ to the signer

Signer:

- computes $\boldsymbol{R_7 = (k_1 + R_5)S}$
- sends $\boldsymbol{R_7}$ to sender

Sender:

- computes $\boldsymbol{= R_8 + bfact \cdot P_{pub}}$

Thus $\boldsymbol{(R_2, R_5, R_8, rx, P)}$ is the ID-based group blind signature of m.

DOI: 01.IJNS.4.1.1133

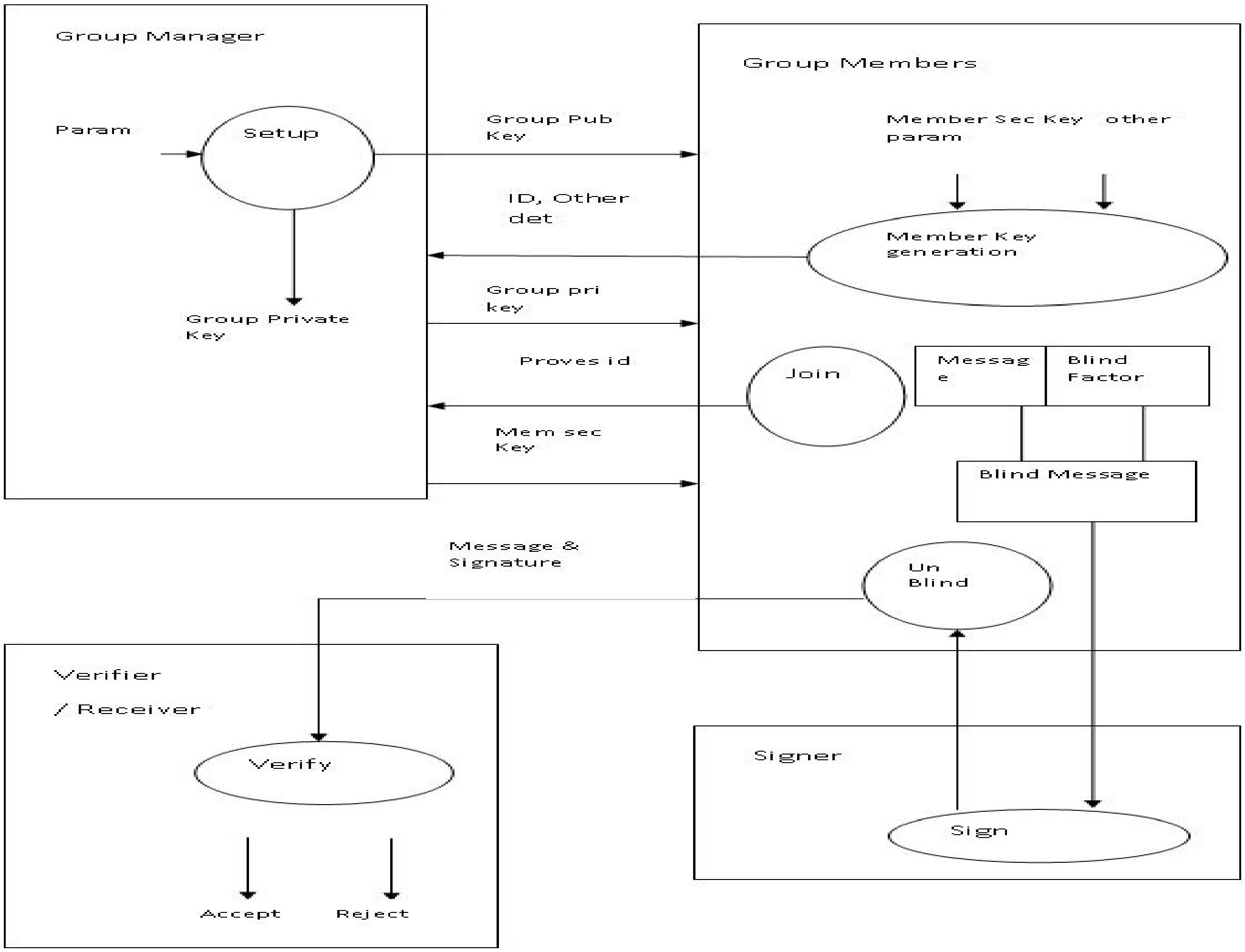

Figure1: Identity based group blind Signature

To produce a group blind signature, the Sender requires three scalar multiplications in G, two hash function evaluation. The Signer requires to compute three scalar multiplications in G and one hash function evaluation.

**Verification:** In this algorithm, the receiver verifies the signature and recovers the message by using the public parameters and the signer's identity. Anyone who knows the public key of the signer can verify the validity of signature with the given a message *m* and its identity based group blind signature.

For a given signature $\boldsymbol{(R_2,R_5,R_8,rx,P)}$

– computes $\boldsymbol{R_6=H_1(m,R_2+R_5)}$
– *computes* $\boldsymbol{H_2(rxP)}$
– verifies if $\boldsymbol{e(R_8,P)= e(R_2+R_6 \cdot H_2(rxP),P_{pub})}$ is valid.

*Proof of verification:*

$$e(R_8,P) \quad = e(R_7+bfact \cdot P_{pub}, P)$$
$$= e(R_7,P)\, e(bfact \cdot P_{pub,} P)$$
$$= e((k_1+R_6)S,P)\, e(bfact \cdot P_{pub,} P)$$
$$= e((k_1+R_6)s \cdot H_2(rxP),P)\, e(bfact \cdot P_{pub,} P)$$
$$= e(k_1 \cdot s \cdot H_2(rxP)+ R_6 \cdot s \cdot H_2(rxP),P)\, e(bfact \cdot P_{pub,} P)$$
$$= e(s \cdot R_1+ R_6 \cdot s \cdot H_2(rxP),P)\, e(bfact \cdot P_{pub,} P)$$
$$= e(R_1+ R_6 \cdot H_2(rxP),sP)\, e(bfact \cdot P_{pub,} P)$$
$$= e(R_1+ R_6 \cdot H_2(rxP), P_{pub})\, e(bfact \cdot P_{pub\,,} P)$$
$$= e(R_1+ R_6 \cdot H_2(rxP), P_{pub})\, e(bfact \cdot P_{,} P_{pub})$$
$$= e(R_1+bfact \cdot P+ R_6 \cdot H_2(rxP), P_{pub})$$
$$= e(R_2+R_6 \cdot H_2(rxP), P_{pub})$$

**Open:**

Given a valid group blind signature, Group Manager can easily identify the signer. The signer cannot refuse the signature after GM gives a zero knowledge proof on given a signature σ of message m. The group manager can identify the originating member by computing Open (master secret key, m, signature), which outputs the identity of the member who created the signature.

The group manager knows for each the identity of the user that is associated with it. This binding is established during the Join phase. As a result, it is easy for a group manager, for a given valid group signature, to determine the identity of the signer.

## V. Conclusion

In this paper we proposed a group blind signature scheme based on the group signature scheme. Our group blind signature scheme is more efficient and secure. The size of the group public key and the group blind signature is independent on the numbers of group members.This method of cryptographic primitive can be used in secured electronic transaction like ecash and evoting where protecting the anonymity of the user is very important. This scheme can be the alternative for traditional blind signature scheme eliminates the need for certificates of public keys required, because public keys are generated from the arbitrary unique identity information.

## References

[1] Barreto, B. Libert, N.McCullagh, and J. Quisquater. Efficient and provably-secure Identity-based signatures and signcryption from bilinear maps. In Proc. of ASIACRYPT05, volume 3778 of LNCS, pages 515-532, 2005.

[2] Boneh.D., M. Franklin, Identity-based Encryption from the Weil pairing , SIAM J. of Computing, 32(3):586-615, 2003. Extended abstract in Advances in Crptology-Crypto'01, LNCS 2139, pp.213-229, Springer-Verlag, 2001

[3] Chaum.D, Blind signature systems, Proceedings of Crypto 83, Springer Verlag, pp.153-158, 1983.

[4] D. Chaum and E. van Heyst, Group signatures, in EUROCRYPT'91, LNCS 547, pp. 257-265, Springer-Verlag, 1991.

[5] D. Boneh, X. Boyen, and H. Shacham, Short group signatures , in CRYPTO'04, LNCS 3152, pp. 45-55, Springer-Verlag, 2004.

[6] Fangguo Zhang, Kwangjo Kim: ID-Based Blind Signature and Ring Signature from Pairings. ASIACRYPT 2002: 533-547

[7] J. Camenisch and A. Lysyanskaya, Signature schemes and anonymous credentials from bilinear maps , in CRYPTO'04, LNCS 3152, pp. 56-72, Springer-Verlag, 2004.

[8] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, A practical and provably secure coalition-resistant group signature scheme , in CRYPTO'00, LNCS 1880, pp. 255-270, Springer-Verlag, 2000.

[9] G. MAITLAND, C. BOYD, Fair electronic cash based on a group signature scheme, Proceedings of ICICS 2001, Lecture Notes in Computer Science, Springer-Verlag, pp. 461-465, 2001.

[10] Gagn.M, Identity-Based Encryption: a Survey, RSA Laboratories Cryptobytes, Vol. 6, No. 1, Spring 2003.

[11] M. Bellare, H. Shi, and C. Zhang, Foundations of group signatures: The case of dynamic groups , in CT-RSA'05, LNCS 3376, pp. 136-153, Springer-Verlag, 2005.

[12] Z. Chen, J. Huang, D. Huang, J. Zhang, and Y.Wang, Provably secure and ID-based group signature scheme ,AINA'04, vol. 02, pp. 384- 387, IEEE, 2004.

[13] S. Zhou and D. Lin, On anonymity of group signatures , in CIS 2005, Part II, LNAI 3802, pp. 131-136, Springer Verlag, 2005.

[14] X. Boyen and B. Waters, Compact group signatures without random oracles. Cryptology ePrint Archive, Report 2005/ 381, 2005.

[15] Shamir.A, Identity-based Cryptosystems and Signature Schemes, In Advances in Cryptology-Crypto'84, LNCS vol. 196, Springer-Verlag, 1984, pp. 47-53.

DOI: 01.IJNS.4.1.1133